UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,068	10/31/2005	Antonius H.M. Akkermans	NL 020645	7468

24737 7590 06/02/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
06/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/519,068	AKKERMANS ET AL.	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/31/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-14* is/are rejected.

7)☒ Claim(s) *6* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/31/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 10/31/2005 but is a 371 case of PCT/IB03/02504 application filed 6/26/2003 and has a foreign priority application filed on 7/5/2002.

Claim Objections

2. Regarding claims 1 – 14, Examiner respectfully suggests the drawing numbers, such as "a first area (3)" as recited in the instant claim, to be removed from the claims to minimize the dependency between the claims and the drawings so that any number changed in the drawing would not mutually impact the other number used in the claims.

3. Claim 4 is objected to because of the following informalities: "for asset en- and decryption" should be "for asset encryption and decryption". Appropriate correction is required.

4. Claim 11 is objected because the claim is dependent on both claim 9 (see Page 19 Line 26) and claim 3 (see Page 19 Line 31). Examiner notes any dependent claim which refers to more than one other claim ("multiple dependent claim") shall refer to such other claims in the alternative way only. See MPEP 608.01(n). Examiner notes for further continuing the prosecution, this examination is assumed to be dependent on claim 9.

5. Claim 12 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. Examiner notes the claim limitations are directed to a device (a record carrier) for decrypting the encrypted payload data that has a group or combination of materials / instruments having a particular function and use such as comprising a first area and a second area and the second area further comprises a chip to store a first counter (C_i) and a second counter (C_e). However, the structural / functional cooperative relationships between the first counter and the second counters on the device (the record carrier) is not recited in the claim. Examiner respectfully requests one of possible claim amendments for resolution, for example, according to the disclosure of the instant application is if the second counter (C_e) is coincided with the first counter (C_i), the payload data E_{AK}(data) is decrypted (SPEC: Page 14 Line 3 – 4).

7. Claims 9 – 11 and 13 are rejected under 35 U.S.C. 112 second paragraph, as being indefinite. Regarding claim 9 and 13, the use of the claim language "optionally" renders these claims indefinite since this phrase leads to a question of whether the claimed operations really occurred and as such merely suggests limitations or makes limitations optional and renders these claims indefinite. Claims 10 – 11 are also rejected by virtue of their dependency.

8. Claim 8 recites the limitation "the manner information" in Page 19 Line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1, 2, 5, 8 – 9 and 11 – 14 are rejected under 35 U.S.C. 102(b) as being anticipated by Ueda et al. (U.S. Patent 6,289,102).

As per claim 1, Ueda teaches a record carrier (Ueda: Figure 5 / Disk 3) having:

a first area storing information (data), which is at least partly stored in encrypted form (E_{AK}(data)), this part being called an asset (E_{AK}(data)) (Ueda: Column 4 Line 14 – 19: a main data field where the scrambled data (i.e. (E_{AK}(data)) is recorded, as taught by Ueda, is considered as a first area), **and which includes a first**

part of decryption information (HCK, E_{DNK}(HCK)) (Ueda: Column 19 Line 16 – 32, Column 40 Line 5 – 6, Column 39 Line 35 – 41 and Column 5 Line 43 – 44: the second key information (i.e. encrypted disk key) is also recorded in the data recording area, as taught by Ueda, and this second key information is encrypted by the bus / master key and is considered as (HCK, E_{DNK}(HCK)), **and the record carrier further having,**

a second area storing a second part of decryption information (UCID) (Ueda: Column 17 Line 45 – 46, Column 4 Line 39 – 41, Column 39 Line 35 – 41, and Column 40 Line 4 – 6: the use identification information is stored in the "sector header" field, which is considered as the second area of the track and the identification information is considered as a UCID); and

both the first (HCK) and second (UCID) parts of decryption information serve in decrypting the asset (E_{AK}(data)) (Ueda: Column 5 Line 4 – 7: descrambles the scrambled data, i.e., E_{AK}(data), based on information obtained by converting the second key information based on the first key information).

As per claim 2, Ueda teaches the first and second areas comprise storage media of a different physical kind (Ueda: Column 40 Line 5 – 6: the lead-in area (i.e. sector header) and the data recording area are considered as two different categories of storage areas).

As per claim 5, Ueda teaches a third cryptographic key, called a hidden-channel key (HCK), serves in the asset decryption, and in that the hidden-channel key (HCK) is

obtainable from the first part of decryption information (HCK, E_{DNK}(HCK)), in particular, that the hidden-channel key (HCK) coincides with the first part of decryption information (HCK) and that the first part of decryption information (HCK) is scrambled and/or encrypted within the information (data) stored in the first area (Ueda: Column 19 Line 16 – 32, Column 40 Line 5 – 6, Column 19 Line 45 – 50: a disk key is considered as a HCK and serves in the asset decryption – it is obtainable from the first part of decryption information (i.e. a encrypted disk key by a master key), and that the first part of decryption information disk key is scrambled / encrypted by a master key and stored in the data recording area (i.e. the first area)).

As per claim 8, Ueda teaches the second area is designed for storing user-specific settings serving in controlling the access of an reading and/or writing device to the record carrier and/or in controlling the manner information being read from the record carrier is presented by the reading and/or writing device to a user of the reading and/or writing device (Ueda: Column 29 Line 43 – 51: the use identification information is stored in the sector header field (i.e. the 2nd area) and compared with reproduction permission information to authorize the reproduction of content data).

As per claim 9 and 13, Ueda teaches a device (Ueda: Figure 22 / Element 1308: a device (i.e. the descrambling circuit) is designed to access the 1st area and 2nd area of data) is designed for reading and/or writing the first part of decryption information (HCK, E_{DNK}(HCK)) (Ueda: Column 19 Line 16 – 32, Column 40 Line 5 – 6, Column 39 Line 35

– 41 and Column 5 Line 43 – 44), for reading and/or writing the second part of decryption information (UCID) (Ueda: Column 17 Line 45 – 46, Column 4 Line 39 – 41, Column 39 Line 35 – 41, and Column 40 Line 4 – 6), for reading and/or writing the asset (E_{AK}(data)), optionally, for obtaining complete decryption information from both the first (HCK, E_{DNK}(HCK)) and second parts (UCID) of decryption information, and, optionally, for decrypting and/or encrypting the asset (E_{AK}(data)) with the complete decryption information (Ueda: Column 5 Line 4 – 7).

As per claim 11, Ueda teaches the device (Ueda: Figure 22 / Element 1308: a device (i.e. the descrambling circuit) is designed to access the 1st area and 2nd area of data) is designed for storing and maintaining a revocation list of identifiers (UCID), and in that the device is designed for at least partly refusing a user of the device access to a record carrier as claimed in claim 3 if the identifier (UCID) being stored on the record carrier belongs to the revocation list (Ueda: Column 29 Line 43 – 51: the use identification information is compared with reproduction permission information to authorize the reproduction of content data and as such the identification information that has the mismatch with he reproduction permission information is considered as falling in a part of the revocation list of identifiers).

As per claim 14, Ueda teaches selecting an identifier (UCID) (Ueda: Column 17 Line 45 – 46 and Column 40 Line 63 – 67: the use identification information the identification information is considered as a UCID), in particular, selecting an identifier

(UCID) being different from the identifiers (UCID) having previously been selected in the method (Ueda: Column 8 Line 39 – 44), constructing the second part of decryption information (UCID) as comprising the identifier (UCID), and producing the record carrier with the thus constructed second part of decryption information (UCID) being stored on the second area of the record carrier (Ueda: Column 17 Line 45 – 46, Column 4 Line 39 – 41, Column 39 Line 35 – 41, and Column 40 Line 4 – 6: the use identification information is stored in the "sector header" field, which is considered as the second area).

As per claim 12, the claim limitations are met as the same reasons as that set forth above in rejecting claim 1.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 3, 4, 7 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueda et al. (U.S. Patent 6,289,102), in view of Kulinets U.S. Patent 6,005,940).

As per claim 3, Ueda does not teach the second area comprises a chip for providing the store of the second area (Ueda: Column 3 Line 1 – 6 / Line 52 – 55: a transponder, fixed to the disk medium, contains a microelectronic chip having secret information embedded therein for deriving a decryption key to decrypt the data content).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kulinets within the system of Ueda because (a) Ueda teaches providing an information recording medium having a security key data structure associated with the medium sector structure (areas) which ensures the prevention of the content recorded in the information recording medium from being illegally copied so as to realize secured copyright protection (Ueda: Column 3 Line 34 – 38) and (b) Kulinets teaches providing a more reliable and effective protection mechanism for an information recording medium by using a self contained deciphering hardware; for example, a transponder, fixed to the disk medium, contains a microelectronic chip having secret information embedded therein for deriving a decryption key to decrypt the data content and this separate embedded hardware device prevents external replicating and analyzing while being able to supply the needed decryption information (Kulinets: Column 3 Line 1 – 6 / Line 52 – 55 and Column 1 Line 63 – Column 2 Line 3).

As per claim 4, Ueda teaches a symmetric method using a first cryptographic key, called an asset key (AK), is used for asset en- and decryption, and in that the asset key (AK) is stored in the second area in an encrypted form, wherein for its encryption a

symmetric encryption method has been used (Ueda: Column 18 Line 2 – 7: the encrypted title key is qualified as an encrypted asset key and is stored in the sector header area (i.e. 2nd area) along with the use identification information (UCID) to descramble the encrypted data).

However, Ueda teaches does not disclose expressly a second cryptographic key (CIDK) in whose derivation both the first (HCK) and second (UCID) parts of decryption information have been used.

Kulinets teaches a second cryptographic key (CIDK) in whose derivation both the first (HCK) and second (UCID) parts of decryption information have been used (Kulinets: Column 6 Line 59, Column 7 Line 14 – 16 and Column 8 Line 26 – 27: (a) the medium data track is divided into frames of encrypted data (b) a deciphering key DK_A along with the frame identification number can be combined to generate another cryptographic key).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kulinets within the system of Ueda because (a) Ueda teaches providing an information recording medium having a security key data structure associated with the medium sector structure (areas) which ensures the prevention of the content recorded in the information recording medium from being illegally copied so as to realize secured copyright protection (Ueda: Column 3 Line 34 – 38) and (b) Kulinets teaches providing an effective and reliable protection mechanism for an information recording medium by using a self contained deciphering hardware and supplying the needed structure of decryption keys on a title by title and a frame by

frame (i.e. sector by sector) basis to allow an authorized user to use the data (Kulinets: Column 2 Line 9 – 11, Column 1 Line 63 – Column 2 Line 3 and Column 3 Line 1 – 2).

As per claim 7, Ueda does not disclose expressly the chip is designed for checking the right of an reading and/or writing device to access the record carrier.

Kulinets teaches the chip is designed for checking the right of and reading and/or writing device to access the record carrier (Kulinets: Column 3 Line 1 – 6, Column 2 Line 25 – 30. Column 7 Line 50 – 59 and Column 8 Line 25 – 28: the chip embedded within the transponder uses a challenge / response protocol to authorize the access to content data where a frame identification number is used as a part of the challenge value).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kulinets within the system of Ueda because (a) Ueda teaches using an identification circuit and identification information before reproduction of the scrambled data is permitted (Ueda: Column 29 Line 42 – 49) and (b) Kulinets teaches providing an effective and reliable protection mechanism by using a separate hardware device such as a chip embedded within the transponder that manages a challenge / response protocol to authorize the access to content data where a frame identification number is also used as a part of the challenge value (Kulinets: Column 3 Line 1 – 6, Column 2 Line 25 – 30. Column 7 Line 50 – 59 and Column 8 Line 25 – 28).

As per claim 10, Ueda does not disclose expressly the device is designed for accessing the first and second areas of the record carrier in parallel.

Kulinets teaches the device is designed for accessing the first and second areas of the record carrier in parallel (Ueda: Column 3 Line 1 – 6 / Line 52 – 55: a transponder, fixed to the disk medium, contains a separate hardware device (i.e. a microelectronic chip) having its own processor and memory so that the first and second areas of the record carrier can be accessed in parallel).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Kulinets within the system of Ueda because (a) Ueda teaches providing an information recording medium having a security key data structure associated with the medium sector structure (areas) which ensures the prevention of the content recorded in the information recording medium from being illegally copied so as to realize secured copyright protection (Ueda: Column 3 Line 34 – 38) and (b) Kulinets teaches providing a more reliable and effective protection mechanism for an information recording medium by using a self contained deciphering hardware; for example, a transponder, fixed to the disk medium, contains a microelectronic chip having secret information embedded therein for deriving a decryption key to decrypt the data content and this separate embedded hardware device provides independent processing with its own processor and memory as well as prevents external replicating and analyzing while being able to supply the needed decryption information (Kulinets: Column 3 Line 1 – 6 / Line 52 – 55 and Column 1 Line 63 – Column 2 Line 3).

Allowable Subject Matter

11. Claim 6 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

The following is an examiner's statement of reasons for allowance: The present invention is directed to a device (a record carrier) for decrypting the encrypted payload data with a first area and a second area, which comprises a chip to store a first counter (C_i) and the second counter (C_e); wherein the second counter (C_e) is stored in an encrypted form and the first (HCK) and second (UCID) parts of decryption information serve in decrypting the second counter (C_e). Both of the closest prior art, U.S. Pattern 6,289,102 and U.S. Pattern 6,005,940, fails to anticipate or render obvious the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/
Longbit Chai Ph.D.
Primary Examiner, Art Unit 2131
5/28/2008